



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,711	10/18/2001	Taizo Shirai	450100-03547	8666

20999 7590 07/12/2005
FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER

KHOSHNOODI, NADIA

ART UNIT PAPER NUMBER

2133

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/982,711

Applicant(s)

SHIRAI ET AL

Examiner

Nadia Khoshnoodi

Art Unit

2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. _____.
 - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendments

Applicant's amendments/arguments filed April 8, 2005 with respect to amended claims 1, 8, 15, 17, 24, 31, & 32 and previously presented claims 2-7, 9-14, 16, 18-23, & 25-30 have been fully considered but are moot in view of the new ground(s) of rejection. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Amendments with regards to claims 1, 8, 15, 17, 24, and 31-32, as filed on 4/8/2005 have been accepted. Therefore, the previous 35 U.S.C. 112, second paragraph rejection has been withdrawn.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Amendments with regards to claims 31-32, as filed on 4/8/2005, have been accepted as curing the previous 35 U.S.C. 101 rejections. Therefore the previous 35 U.S.C. 101 rejections with regards to these claims have been withdrawn.

Response to Arguments

Applicant contends that Hazard does not disclose or suggest an information recording device wherein "a block permission table for accessing a permission table that describes memory access control information." Examiner respectfully disagrees. Hazard teaches a "Number of Associated Key" in col. 2 of Fig. 3 which can be used in combination with Fig. 2, col.2 "Key Number" in order to gain access to the "Key Stored Value," col. 4 of Fig. 2 which can be construed as the permission that controls access to the sensitive data, i.e. describes memory access control information. Furthermore, Hazard also teaches that the encryption key is used in order to gain access to the sensitive information (col. 5, lines 18-39). Therefore, Hazard teaches the claimed limitation of the device wherein "a block permission table for accessing a permission table that describes memory access control information."

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

II. Claims 1-2, 5, 8, 15-18, 21, 24-25, 28, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hazard, United States Patent No. 6,658,566 and further in view of Harada United States Patent No. 6,850,914.

As per claims 1 and 17:

Hazard substantially teaches an information recording device and method for executing

Art Unit: 2133

processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said information recording device comprising a cryptosystem unit which selectively uses different encryption keys for each sectors from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors (col. 5, lines 1-14 and fig. 2). Furthermore, Hazard also teaches a block permission table for accessing a permission table that describes memory access control information (fig. 2, col. 2 "Key Number" used to gain information about the "Key Stored Value" associated with fig. 3, col. 2 "Number of Associated Key").

Also taught by Hazard is a unique reference associated with each piece of sensitive information (fig. 3, col. 1 "Reference of Sensitive Information"), which Hazard teaches can be any information a person would want to keep confidential (col. 1, lines 35-38). Not explicitly disclosed is wherein the memory stores content and media identifier data unique to each media. However, Harada et al. teach that there is indeed a need to develop technologies to prevent from those who violate copyright laws. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard for the sensitive information to be a form of media. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Harada et al. in col. 1, lines 19-33.

As per claims 2 and 18:

Hazard and Harada et al. substantially teach an information recording device and method

Art Unit: 2133

of claim 1. Furthermore, Hazard teaches the information recording device and method wherein in said cryptosystem unit, from among M different encryption keys corresponding to M sectors, which are stored in header information corresponding to the data to be stored in said memory, one encryption key is selected in accordance with a sector in which the data is stored, and the selected encryption key is used to perform the encryption of data to be stored in each of the sectors (col. 5, lines 35-39 and fig. 3). Although the term "header information" is not specifically used, the information is stored in such a way that it is identical to that of header information.

As per claims 5 and 21:

Hazard and Harada et al. substantially teach an information recording device and method of claim 1. Furthermore, Hazard teaches the information recording device and method wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as single-DES encryption processing using different encryption keys for the sectors (col. 4, lines 32-46).

As per claims 8 and 24:

Hazard substantially teaches the information recording device and method for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said information playback device comprising a cryptosystem unit which selectively uses different decryption keys for the first sector to M-th sector to execute decryption processing and which executes decryption processing on data stored in each of the sectors (col. 4, lines 32-46,

Art Unit: 2133

col. 5, lines 1-14, and fig. 2). Furthermore, Hazard also teaches a block permission table for accessing a permission table that describes memory access control information (fig. 2, col. 2 “Key Number” used to gain information about the “Key Stored Value” associated with fig. 3, col. 2 “Number of Associated Key”).

Also taught by Hazard is a unique reference associated with each piece of sensitive information (fig. 3, col.1 “Reference of Sensitive Information”), which Hazard teaches can be any information a person would want to keep confidential (col. 1, lines 35-38). Not explicitly disclosed is wherein the memory stores content and media identifier data unique to each media. However, Harada et al. teach that there is indeed a need to develop technologies to prevent from those who violate copyright laws. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard for the sensitive information to be a form of media. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Harada et al. in col. 1, lines 19-33.

As per claims 9 and 25:

Hazard and Harada et al. substantially teach an information recording device and method of claim 8. Furthermore, Hazard teaches the information recording device and method wherein, in said cryptosystem unit, from among M different decryption keys corresponding to M sectors, which are stored in header information corresponding to data stored in said memory, one decryption key is selected in accordance with a sector in which the data is stored, and the selected decryption key is used to perform the decryption of data stored in each of the sectors (col. 4, lines 32-46; col. 5, lines 35-39 and fig. 3). Although the term “header information” is not

Art Unit: 2133

specifically used, the information is stored in such a way that it is identical to that of header information.

As per claims 12 and 28:

Hazard and Harada et al. substantially teach an information recording device and method of claim 8. Furthermore, Hazard teaches an information playback device and method wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as single-DES decryption processing using different decryption keys for the sectors (col. 4, lines 32-46).

As per claim 15:

Hazard substantially teaches an information recording medium having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), wherein a plurality of different cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area (col. 5, lines 35-39). Although the term "header information" is not specifically used, the information is stored in such a way that it is identical to that of header information. Furthermore, Hazard also teaches a block permission table for accessing a permission table that describes memory access control information (fig. 2, col. 2 "Key Number" used to gain information about the "Key Stored Value" associated with fig. 3, col. 2 "Number of Associated Key").

Also taught by Hazard is a unique reference associated with each piece of sensitive information (fig. 3, col. 1 "Reference of Sensitive Information"), which Hazard teaches can be any information a person would want to keep confidential (col. 1, lines 35-38). Not explicitly

Art Unit: 2133

disclosed is wherein the memory stores content and media identifier data unique to each media.

However, Harada et al. teach that there is indeed a need to develop technologies to prevent from those who violate copyright laws. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard for the sensitive information to be a form of media. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Harada et al. in col. 1, lines 19-33.

As per claim 16:

Hazard and Harada et al. substantially teach an information recording device and method of claim 15. Furthermore, Hazard teaches an information recording medium, wherein said plurality of different cryptographic keys are M different encryption keys corresponding to the M sectors (col. 5, lines 1-14 and fig. 2).

As per claim 31:

Hazard substantially teaches a program providing medium for providing a computer program which controls a computer system to execute processing which stores data in a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said computer program comprising a data-encrypting step in which encryption processing on data to be stored in the sectors is executed by performing encryption using encryption keys selected for the first sector to the M-th sector (col. 5, lines 1-14 and fig. 2). Furthermore, Hazard also teaches a block permission table for accessing a permission table that describes memory access control information (fig. 2, col. 2 "Key

Art Unit: 2133

Number” used to gain information about the “Key Stored Value” associated with fig. 3, col. 2 “Number of Associated Key”).

Also taught by Hazard is a unique reference associated with each piece of sensitive information (fig. 3, col.1 “Reference of Sensitive Information”), which Hazard teaches can be any information a person would want to keep confidential (col. 1, lines 35-38). Not explicitly disclosed is wherein the memory stores content and media identifier data unique to each media. However, Harada et al. teach that there is indeed a need to develop technologies to prevent from those who violate copyright laws. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard for the sensitive information to be a form of media. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Harada et al. in col. 1, lines 19-33.

As per claim 32:

Hazard substantially teaches program providing medium for providing a computer program which controls a computer system to execute processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said computer program comprising a data-decrypting step in which decryption of data stored in each of the sectors is performed by executing decryption processing using decryption keys selected in accordance with the first sector to the M-th sector (col. 4, lines 32-46, col. 5, lines 1-14, and fig. 2). Furthermore, Hazard also teaches a block permission table for accessing a permission table that describes memory

Art Unit: 2133

access control information (fig. 2, col. 2 "Key Number" used to gain information about the "Key Stored Value" associated with fig. 3, col. 2 "Number of Associated Key").

Also taught by Hazard is a unique reference associated with each piece of sensitive information (fig. 3, col.1 "Reference of Sensitive Information"), which Hazard teaches can be any information a person would want to keep confidential (col. 1, lines 35-38). Not explicitly disclosed is wherein the memory stores content and media identifier data unique to each media. However, Harada et al. teach that there is indeed a need to develop technologies to prevent from those who violate copyright laws. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard for the sensitive information to be a form of media. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Harada et al. in col. 1, lines 19-33.

III. Claims 3-4, 6, 10-11, 13, 19-20, 22, 26-27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hazard, United States Patent No. 6,658,566 and Harada et al., United States Patent No. 6,850,914 as applied to claims 1, 8, 17, and 24 above, and further in view of Dilkie et al., United States Patent No. 6,341,164.

As per claims 3 and 19:

Hazard and Harada et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the device/method wherein, in said cryptosystem unit, from among M different encryption keys corresponding to M sectors, which are stored in header information corresponding to the data to be stored in said memory, a set of at least two encryption keys is selected in accordance with a sector in which the

Art Unit: 2133

data is stored, and the selected encryption keys are used to perform the encryption of data to be stored in each of the sectors. However, Hazard teaches the use of single-DES encryption (col. 4, lines 32-46). Furthermore, Dilkie et al. teach the use of triple-DES which uses at least 2 keys for encryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the encryption processing, thereby using at least 2 keys for encryption. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54. As per claims 4 and 20:

Hazard and Harada et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the device/method wherein, in said cryptosystem unit, from among P different encryption keys in which the number P differs from the number M, at least one encryption key is selected in accordance with a sector in which the data is stored, and the selected at least one encryption key is used to perform the encryption of data to be stored in each of the sectors.

However, Dilkie et al. teach that from among P different encryption keys, where P differs from the number M, at least one encryption key is selected from a key package to use for encryption purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to choose at least one encryption key for encrypting data to be stored in each of the sectors from P different keys, where the number P differs from the number M. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have

Art Unit: 2133

been motivated to do so since it is suggested by Dilkie et al. in col. 4, lines 1-37 and col. 4, line 51- col. 2, line 6.

As per claims 6 and 22:

Hazard and Harada et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the information recording device wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as triple-DES encryption processing using at least two different encryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES encryption processing. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the encryption processing. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 10 and 26:

Hazard and Harada et al. substantially teach an information playback device and method, as applied to claims 8 and 24 above. Not explicitly disclosed is the device/method wherein an information playback device and method wherein, in said cryptosystem unit, from among M different decryption keys corresponding to M sectors, which are stored in header information corresponding to data stored in said memory, a set of at least two decryption keys is selected in accordance with a sector in which data is stored, and the selected encryption keys are used to perform the decryption of data stored in each of the sectors. However, Hazard teaches the use of single-DES decryption (col. 4, lines 32-46 and col. 4, lines 32-46). Furthermore, Dilkie et al.

Art Unit: 2133

teach the use of triple-DES which uses at least 2 keys for decryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the decryption processing, thereby using at least 2 keys for decryption. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 11 and 27:

Hazard and Harada et al. substantially teach an information playback device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the device/method wherein, in said cryptosystem unit, from among P different decryption keys in which the number P differs from the number M, at least one decryption key is selected in accordance with a sector in which data is stored, and the selected at least one decryption key is used to perform the decryption of data stored in each of the sectors.

However, Dilkie et al. teach that from among P different encryption keys, where P differs from the number M, at least one encryption key is selected from a key package to use for encryption purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to choose at least one decryption key based on the encryption keys stored in each of the sectors from P different keys, where the number P differs from the number M. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 4, lines 1-37, col. 4, line 51-col. 2, line 6, and col. 5, lines 61-67).

Art Unit: 2133

As per claims 13 and 29:

Hazard and Harada et al. substantially teach an information playback device and method, as applied to claims 8 and 24 above. Not explicitly disclosed by Hazard is the information playback device wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as triple-DES decryption processing using at least two different decryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES decryption processing. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the decryption processing. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

IV. Claims 7, 14, 23, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hazard, United States Patent No. 6,658,566 and Harada et al., United States Patent No. 6,850,914 as applied to claims 1, 8, 17, and 24 above, and further in view of Schneier, *Applied Cryptography*.

As per claims 7 and 23:

Hazard and Harada et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Furthermore, Hazard teaches the use of header information used to store the key as encrypted by an encryption algorithm, as well as other relevant information (col. 8, lines 15-39). Not explicitly disclosed by Hazard is the device/method wherein said cryptosystem unit selectively executes one of sector-independent encryption processing in which in accordance with an encryption format type stored in header

Art Unit: 2133

information corresponding to the data to be stored in said memory, the entirety of the data is encrypted in a single encryption mode, and sector-dependent encryption processing in which in accordance with the encryption format type, the data is encrypted by using encryption keys which are selected for the sectors.

However, Schneier teaches using sector-independent encryption processing where the entirety of data is encrypted in a single encryption mode, and sector-dependent encryption processing where the data is encrypted by using encryption keys that are selected for the sectors. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to store the encryption format type in the header information to designate a sector-dependent or sector-independent encryption format. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Schneier on pages 221, lines 8-12 and 222, lines 24-43.

As per claims 14 and 30:

Hazard and Harada et al. substantially teach an information playback device and method, as applied to claims 8 and 24 above. Furthermore, Hazard teaches the use of header information used to store the key as encrypted by an encryption algorithm, as well as other relevant information (col. 8, lines 15-39). Not explicitly disclosed by Hazard is the device/method wherein said cryptosystem unit selectively executes one of sector-independent decryption processing in which in accordance with an encryption format type stored in header information corresponding to data stored in said memory, the entirety of the data is decrypted in a single decryption mode, and sector-dependent decryption processing in which in accordance with the

Art Unit: 2133

encryption format type, the data is decrypted by using decryption keys which are selected for the sectors.

However, Schneier teaches using sector-independent decryption processing where the entirety of data is decrypted in a single decryption mode, and sector-dependent decryption processing where the data is decrypted by using decryption keys that are selected for the sectors. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to store the encryption format type in the header information to designate a sector-dependent or sector-independent decryption format. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Schneier on pages 221, lines 8-12 and 222, lines 24-43.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2133

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825.

The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.



Nadia Khoshnoodi
Examiner
Art Unit 2133
7/8/05

NK



DAVIDTON
PRIMARY EXAMINER